# K. K. Wagh Polytechnic, Nashik

# QUESTION BANK

## Unit Test-II

**Course Title: -Emerging Trends in Computer and Info. Tech.**

**Course Abbr & Code:-ETI (22618)**

---

**MULTIPLE CHOICE QUESTIONS AND ANSWERS**

---

## Chapter 4- Digital Forensics (CO4)

1._____ plays vital role in criminal justice systems
- **a) Forensics science**
- b) Digital evidences
- c) Volatile Evidence
- d) All of the Above

2. Digital forensics is all of them except:
- a) Extraction of computer data.
- b) Preservation of computer data.
- c) Interpretation of computer data.
- **d) Manipulation of computer data.**

3. Which of following is not a rule of digital forensics?
- **a) An examination should be performed on the original data**
- b) A copy is made onto forensically sterile media
- c) The copy of the evidence must be an exact, bit-by-bit copy
- d) The chain of custody of all evidence must be clearly maintained

4. IDIP stands for:
- **a) Integrated Digital Investigation Process.**
- b) Integrated Data Investigator Process.
- c) Integrated Digital Investigator Process.
- d) Independent Digital Investigator Process

5. Who is the father of Computer Forensics?
- a) G.Palmar
- **b) Michael Anderson**
- c) S.Ciardhuain
- d) Carrier and Safford

6. Who proposed Abstract Digital Forensic model (ADFM)
- **a) Reith, Carr, Gunsh**
- b) S.Ciardhuain
- c) Carrier and Safford
- d) G.Palmar

7.A valid definition of digital evidence is:_____

a) Data stored or transmitted using a computer
b) Information of probative value
c) **Digital data of probative value**
d) Any digital evidence on a computer

8. Which of following is not general ethical norm for Investigator?
a) To contribute to society and human being.
**b) To express an opinion on the guilt or innocence belonging to any party**
c) To be honest and trustworthy.
d) To honor confidentially.

9. Which of following is a not unethical norm for Digital Forensics Investigation?
a) Uphold any relevant evidence.
b) Declare any confidential matters or knowledge.
c) Distort or falsify education, training, credentials.
**d) Should be fair and take action not to discriminate.**

10. Digital Forensics entails ……
a) Accessing the system's directories viewing mode and navigating through the various systems files and folders
b) Undeleting and recovering lost files
c) Identifying and solving computer crimes
**d) The identification, preservation, recovery, restoration and presentation of digital evidence from systems and devices**

11 The digital evidence are used to establish a credible link between…….
**a) Attacker and victim and the crime scene**
**b)** Attacker and the crime scene
**c)** Victim and the crime scene
**d)** Attacker and Information

12. Digital evidences must follow the requirements of the …….
a) Ideal Evidence rule
**b) Best Evidence rule**
c) Exchange rule
d) All of the above

13. Which property defines evidence must be usable in the court.
**a) Admissible**
**b)** Authentic
**c)** Complete
**d)** Reliable

14. The criminological principle which states that, when anyone, or anything, enters a crime scene he/she takessomething of the scene with him/her, and leaves something of himself/herself behind, is:
**a) Locard's Exchange Principle**
**b)** Differential Association Theory
**c)** Beccaria's Social Contract
**d)** None of the above

15. When an incident takes place, a criminal will leave hint evidence at the scene and remove a hint from the scene which is called as ……..
**a) Locard's Exchange principle**
**b)** Anderson's Exchange principle

**c)** Charles's Anthony principle
**d)** Kevin Ashton principle

16. The evidences or proof that can be obtained from the electronic source is called as……..
**a) Digital evidence**
**b)** Demonstrative evidence
**c)** Explainable evidence
**d)** Substantial evidence

17. Photographs, videos, sound recordings, X-rays, maps, drawing, graphs, and charts are examples is a type of which .
a) Electronic evidence
b) Illustrative evidence
c) Documented evidence
d) Explainable evidence

18. For an evidence to be admissible, it is necessary that it should be……..
a) Complete
**b) Authenticated**
c) Reliable
d) Believable

19. The process of ensuring that providing the data that you have collected is similar to the data presented in a court is known as……
a) Evidence verification
**b) Evidence validation**
c) Evidence authentication
d) Best evidence

20. Which of following is a most volatile evidence source?
a) Main memory
b) Temporary file systems
**c) Registers and cache**
d) Secondary memory

21. Which of the following is not a type of volatile evidence?
a) Routing tables
b) Main memory
**c) Log files**
d) Cached data

22. Which of following are rule of digital forensics?
a) An examination should never be performed on the original data
b)The copy of the evidence must be an exact, bit-by-bit copy
c)The chain of custody of all evidence must be clearly maintained
**d) All of the Above**

**23.** Which phase provides a mechanism for an incident to be detected and confirmed?
a) Readiness phase
b**) Deployment phase**
c) Physical Crime Investigation phase
d) Digital Crime Investigation phase

## Chapter 5: Basics of Hacking (CO5)

1. Ethical Hacking is also known as …….
   a) Black Hat Hacking.
   **b) White Hat Hacking.**
   c) Gray Hat Hacking
   d) Script kiddies

2. Hackers which are invited by software vendors to find security flaws are_____
   a) **White Hat Hackers**
   b) Gray Hat Hackers
   c) Black Hat Hackers
   d) Blue Hat Hackers

3. Vulnerability scanning in Ethical hacking finds……...
   a) Strengths.
   **b) Weakness.**
   c) Both a and b
   d) None of these.

4. Sequential step hacker's use are _____.
   1. Maintaining Access.
   2. Reconnaissance
   3. Gaining Access.
   4. Scanning
   a) 2, 3, 4,1
   b) 4, 2, 3, 1
   **c) 2, 4, 3, 1**
   d) 4, 3, 2, 1

5. What is social engineering?

   a) A technique to identify vulnerabilities in a system or network
   b) A technique to exploit vulnerabilities in a system or network
   **c) A technique to manipulate people into giving up sensitive information**
   d) A technique to fix vulnerabilities in a system or network

6. The term cracker refers to…….
   a) **Black hat hacker**.
   b) White hat hacker.
   c) Grey hat hacker.
   d) None of the above.

7. Who described a dissertation on fundamentals of hacker's attitude?
   a) G. Palma.
   **b) Raymond.**
   c) Either.
   d) Jhon Browman.

8. Which type of hackers hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse?
   a) Black Hat Hacker.
   b) Gray Hat Hacker
   **c) Ethical Hacker**
   d) Script kiddies

9. Which type of hackers uses hacking to send social, religious, and political, etc. messages?
   a) White Hat Hacker
   b) Black Hat Hacker
   **c) Hacktivist**
   d) Script kiddies

10. Which type of hacker hacks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner?
   a) White Hat Hacker
   b) Black Hat Hacker
   **c) Gray Hat Hacker**
   d) Hacktivist
   e) Script kiddies

11. Security audits are usually based on……..
   a) Entries.
   **b) Checklists.**
   c) Both a and b
   d) None of the above

12. Ethical hacking is also known as ……
   a) Penetration testing.
   b) Intrusion testing.
   c) Red teaming.
   **d) All of the above.**

13. What is main goal of ethical hacking?
   a) To cause damage to system
   b) To gain unauthorized access to a system
   **c) To identify and fix security vulnerabilities**
   d) To steal sensitive information

14 ……is similar to a backup, but it is a complete image of a protected system, including data and system files.
   a) Replication
   b) Backup
   **c) Snapshots**
   d) DPLR

15 Data subjects can ask data controllers to "forget" their personal data is…….
   **a) Right to erasure**
   b) Automated decision making
   c) Transferring data outside the EU
   d) Right to Control

16. Which entity that holds or processes personnel data on behalf of another organization?
   a. GDPR Data Controller
   **b. GDPR Data Processor**
   c. Data Protection Officer
   d. All of the Above

17. _____involves automating the transmission of critical data to offline and online storage.
   a) Data availability
   **b) Data lifecycle management**
   c) Information lifecycle management
   d) All of the Above

18. To connecting into network through a rogue modem attached to computer behind a firewall is an example ofwhich type of attack?
   a. Nontechnical attacks
   **b. Network infrastructure attack**
   c. Operating system attack
   d. Application and other specialized attack

19. Breaking file system security is an example of which type of attack?
   a. Nontechnical attacks
   b. Network infrastructure attack
   **c. Operating system attack**
   d. Application and other specialized attack

20. Malicious software includes……..
   a. Viruses
   b. Worms,
   c. Trojan horses
   **d. All of the Above**

21. Which tool is used to crack password?
   **a)** Ethereal
   **b)** Nmap
   **c)** Whisker
   **d) LC4**

22. Which tool is used for depth analysis of a web application?
   a) Ethereal
   b) Nmap
   **c) Whisker**
   d) LC4

23. The Information Technology Act 2000 is an Act of Indian Parliament notified on……..
   a) 27th October 2000
   b) 15th December 2000
   c) 17th November 2000
   **d) 17th October 2000**

24. The offense “Receiving stolen computer or communication device” comes under ……section of Cybersecurity Act 2000.
   **a) 66B**
   b) 67A
   c) 66E
   d) 66C

25. The offense “Failure /refusal to decrypt data” comes under.....section of Cyber security Act 2000.
a) 68
**b) 69**
c) 70
d) 71

26. Which section penalized sending "offensive messages"?
**a) Section 66A**
b) Section 66B
c) Section 66C
d) Section 66D

27. Data subjects can ask data controllers to “forget” their personal data is…….
a) **Right to erasure**
b) Automated decision making
c) Transferring data outside the EU
d) Right to Control

28. To connecting into network through a rogue modem attached to computer behind a firewall is an example of which type of attack?
a) Nontechnical attacks
b) **Network infrastructure attack**
c) Operating system attack
d) Application and other specialized attack

29. Which tool is used to crack password?
a) Ethereal b) Nmap c) Whisker d) **LC4**

30. What is main goal of ethical hacking?
a) To cause damage to system
b) To gain unauthorized access to a system
c**) To identify and fix security vulnerabilities**
d) To steal sensitive information

**Chapter -6 : Types of Hacking (CO6)**

---

1. SNMP stands for……..
a) Simple Network Messaging Protocol
b) Simple Network Mailing Protocol
**c) Simple Network Management Protocol**
d) Simple Network Master Protocol

2. Which of the following tool is used for Network Testing and port Scanning……..
a) NetCat
b) SuperScan
c) NetScan
**d) All of above**

3. Banner grabbing is mostly used for…….
**a) White Hat Hacking**
b) Black Hat Hacking

c) Grey Hat Hacking
d) Script Kiddies

4. An attacker can create an .....attack by sending hundreds or thousands of e-mails a with very large attachments.

a) Connection Attack
**b) Auto responder Attack**
c) Attachment Overloading Attack
d) All the above

5. Which of the following tool is used for Windows for network queries from DNS lookups to trace routes?

**a) Sam Spade**
b) SuperScan
c) NetScan
d) Netcat

6. Which tool is used for ping sweeps and port scanning?

a) Netcat

b) SamSpade
**c) SuperScan**
d) All the above

7. Which of the following tool is used for security checks as port scanning and firewall testing?
**a) Netcat**
b) Nmap
c) Data communication
d) Netscan

8. What is the most important activity in windows vulnerabilities?
a) Information gathering
**b) Cracking password**
c) Escalating privileges
d) Covering tracks

9. What is purpose of Denial of Service attacks?
a) Exploit weakness in TCP/IP attack.
b) To execute a Trojan horse on a system.
**c) To overload a system so it is no longer operational.**
d) To shutdown services by turning them off.

10. What port does Telnet use?
a) 22
b) 80
c) 20
**d) 23**

11. An excessive amount of ARP requests can be a sign of an .....attack on your network.
**a) ARP poisoning attack**
b) ARP Sniffing attack
c) MAC-address poisoning
d) MAC-address Sniffing

12. ARP spoofing is often referred to as……..

a) Denial-of-Service attack
**b) Man-in-the-Middle attack**
c) Sniffing attack
d) Flooding attack

14 Attack, which can take down your Internet connection or your entire network.

a) MAC
**b) DOS**
c) IDS
d) None of above

16. What are the port states determined by Nmap?
a) Active, inactive, standby
b) Open, half-open, closed
**c) Open, closed, filtered**
d) Active, closed, unused

17 .....include phishing, SQL injection, hacking, social engineering, spamming, denial ofservice attacks, Trojans, virus and worm attacks.

a) Operating system vulnerabilities
b) Web vulnerabilities
c) Wireless network vulnerabilities
**d) Network infrastructure Vulnerabilities**

18. Which protocol plays important role in MAC –daddy attack?

**a) ARP**
**b)** FTP
**c)** SMTP
**d)** SNMP

19. "allintitle" Google dork operator returns

**a) results for pages that meet all of the keyword criteria**
**b)** pages with specific text in their HTML title
**c)** matches for URLs that meet all the matching criteria
**d)** specific files containing title

22 .....is a technique used by hackers to find the information exposed accidentally to the internet.

a) Buffer overflow
**b) Google Dorking**
c) Google Shadow
d) GDPR

23. What is ARP poisoning or spoofing?
**a)** It is a method of stealing personal data
**b) It is a type of man-in-the-middle (MITM) attack**
**c)** It is a way to bypass firewalls
**d)** It is a technique used to perform DDoS attacks

24. How can hackers modify ARP tables?
**a)** By using a proxy server
**b) By running a program such as dsniff or Cain & Abel**
**c)** By brute-forcing the network password
**d)** By launching a phishing attack

25. What is a buffer-overflow attack?
a) An attack that causes a program to stop functioning
b) An attack that fills up the hard drive with useless data
**c) An attack that sends extra data to a program's buffer to corrupt or overwrite adjacent data**
d) An attack that steals personal data from a program's buffer

26. What is the impact of excessive retention of sensitive data in database management systems?
**a)** It reduces the impact of a security breach
**b) It increases the impact of a security breach**
**c)** It has no impact on the security breach
**d)** It helps prevent security breaches

27. What is SQL injection?

**a)** A technique to identify vulnerabilities in a system or network
**b)** **A technique to exploit vulnerabilities in a system or network**
**c)** A technique to fix vulnerabilities in a system or network
**d)** A technique to steal sensitive information from a system or network

28. Email bomb can crash a server and provide .....administrator access
**a)** Authorized
**b)** **Unauthorized**
**c)** Both A and B
**d)** None of the above

29. Hackers attacks against insecure Web Application via…….
**a)** **HTTP**
**b)** FTP
**c)** HTTPS
**d)** UDP

30. SQL Injection is which type of vulnerability?
**a)** Web Application vulnerability
**b)** **Security vulnerability**
**c)** Windows vulnerability
**d)** All of the above

31. Google Dorking is also known as…….
**a)** Google Tracking
**b)** **Google Hacking**
**c)** Google fetching
**d)** None of the above

32. Which of the following is/are Google Dork operator?
**a)** intitle
**b)** allintitle
**c)** inurl
**d)** **All of the above**

33. What is the intitle operator in Google Dorks?

a) It allows a hacker to search for pages based on the text contained in the URL
**b)** **It searches for specific text in the HTML title of a page**
c) It helps a hacker narrow down search results to specific file types
d) It searches for files based on their file extension.

34. What is the inurl operator in Google Dorks?

**a)** **It allows a hacker to search for pages based on the text contained in the URL**
**b)** It searches for specific text in the HTML title of a page
**c)** It helps a hacker narrow down search results to specific file types
**d)** It searches for files based on their file extension

.
What is the purpose of the filetype operator in Google Dorks?

**e)** To search for pages with specific text in their HTML title
**f)** To search for pages based on the text contained in the URL

**g) To help a hacker narrow down search results to specific file types**
**h)** To search for files based on their file extension

35. What is the intext operator in Google Dorks?

**a)** It allows a hacker to search for pages based on the text contained in the URL
**b)** It searches for specific text in the HTML title of a page
**c)** It helps a hacker narrow down search results to specific file types
**d) It searches the entire content of a given page for keywords supplied by the hacker**

36. Which operator allows a hacker to search for pages based on the text contained in the URL?

**a)** intitle
**b)** allintitle
**c) inurl**
**d)** allinurl

37. Which operator searches the entire content of a given page for keywords supplied by the hacker?

**a)** intitle
**b)** allintitle
**c) intext**
**d)** allintext

38. What are some common vulnerability found in all versions of Windows?

**a)** DoS, Remote Code Execution, and SQL Injection
**b)** Buffer Overflow, Cross-site Scripting, and Directory Traversal.
**c)** CSRF File Inclusion, Http Response Splitting, and Gain Information/Privileges.
**d) All of the above.**

39. Why is Microsoft Windows OS the most widely hacked?

**a)** Because Microsoft doesn't care about security as much as other OS vendors.
**b)** Because it has the most vulnerabilities.
**c) Because it is the most widely used OS in the world.**
**d)** None of the above.

40. What type of vulnerability was used by the Blaster worm in UNIX and Linux systems?

**a)** DoS.
**b)** Remote Code Execution.
**c) Remote Procedure Call**
**d)** SQL Injection.